(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005年8月18日 (18.08.2005)

PCT

(10) 国際公開番号
WO 2005/076520 A1

(51) 国際特許分類[7]: H04L 9/12, H03M 13/09, 13/19

(21) 国際出願番号: PCT/JP2004/001389

(22) 国際出願日: 2004年2月10日 (10.02.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目2番3号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 松本 渉 (MATSUMOTO, Wataru) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内 Tokyo (JP).

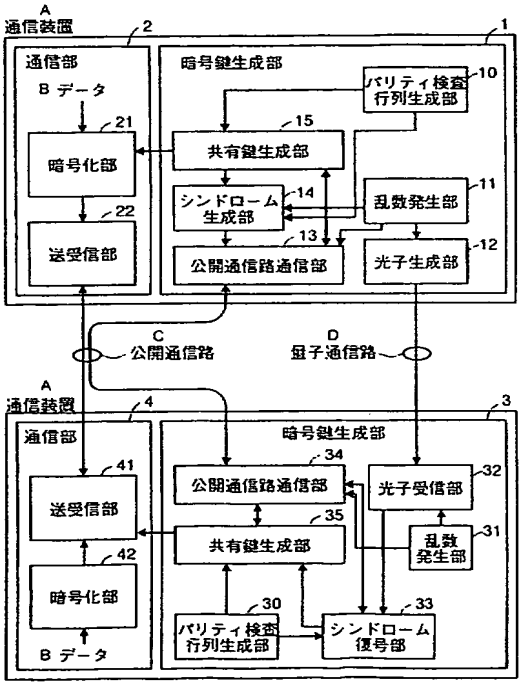
(74) 代理人: 酒井 宏明 (SAKAI, Hiroaki); 〒1000013 東京都千代田区霞が関三丁目2番6号 東京倶楽部ビルディング 酒井国際特許事務所 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[続葉有]

(54) Title: QUANTUM KEY DELIVERING METHOD AND COMMUNICATION DEVICE

(54) 発明の名称: 量子鍵配送方法および通信装置



A...COMMUNICATION DEVICE
2...COMMUNICATION UNIT
B... DATA
21...ENCRYPTING SECTION
22...TRANSMITTING/RECEIVING SECTION
1...ENCRYPTION KEY GENERATING UNIT
15...SHARED KEY GENERATING SECTION
14...SYNDROME GENERATING SECTION
13...OPEN COMMUNICATION PATH COMMUNICATION SECTION
10...PARITY CHECK MATRIX GENERATING SECTION
11...RANDOM NUMBER GENERATING SECTION
12...PHOTON GENERATING SECTION
C...OPEN COMMUNICATION PATH
D...QUANTUM COMMUNICATION PATH
4...COMMUNICATION UNIT
41...TRANSMITTING/RECEIVING SECTION
42...ENCRYPTING SECTION
3...ENCRYPTION KEY GENERATING UNIT
34...OPEN COMMUNICATION PATH COMMUNICATION SECTION
35...SHARED KEY GENERATING SECTION
32...PHOTON RECEIVING SECTION
31...RANDOM NUMBER GENERATING SECTION
30...PARITY CHECK MATRIX GENERATING SECTION
33...SYNDROME DECRYPTING SECTION

(57) Abstract: A quantum key delivering method in which an error in received data is corrected by a check matrix for the determinate stable-characteristic "Irregular-LDPC code", and a part of shared information is discarded according to opened error correction information. Another mode of quantum key delivering method in which while lowering the code rate until the errors in the received data are perfectly corrected, a parity check matrix corresponding to a specific code rate is extracted from the parity check matrices optimized at code rates in a desired range, an additional syndrome is generated, and an error correction processing is repeated using the additional syndrome.

[続葉有]

WO 2005/076520 A1

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: 本発明にかかる量子鍵配送方法においては、確定的で特性が安定した「Ｉｒｒｅｇｕｌａｒ−ＬＤＰＣ符号」用の検査行列を用いて受信データの誤りを訂正し、公開された誤り訂正情報に応じて共有情報の一部を捨てることとした。また、本発明にかかる量子鍵配送方法においては、受信データの誤りを完全に訂正できるまで、符号化率を下げながら、所望の範囲の符号化率で最適化されたパリティ検査行列から特定の符号化率に対応したパリティ検査行列を抽出し、さらに追加のシンドロームを生成し、この追加シンドロームを用いて誤り訂正処理を繰り返し実行することとした。

明　細　書

量子鍵配送方法および通信装置

技術分野

本発明は、高度に安全性の保証された共通鍵を生成することが可能な量子鍵配送方法に関するものであり、特に、誤り訂正符号を用いてデータ誤りを訂正可能な量子鍵配送方法および当該量子鍵配送を実現可能な通信装置に関するものである。

背景技術

以下、従来の量子暗号システムについて説明する。近年、高速大容量な通信技術として光通信が広く利用されているが、このような光通信システムでは、光のオン／オフで通信が行われ、オンのときに大量の光子が送信されているため、量子効果が直接現れる通信系にはなっていない。

一方、量子暗号システムでは、通信媒体として光子を用い、不確定性原理等の量子効果が生じるように１個の光子で１ビットの情報を伝送する。このとき、盗聴者が、その偏光，位相等の量子状態を知らずに適当に基底を選んで光子を測定すると、その量子状態に変化が生じる。したがって、受信側では、この光子の量子状態の変化を確認することによって、伝送データが盗聴されたかどうかを認識することができる。

第１９図は、従来の偏光を利用した量子鍵配送の概要を示す図である。たとえば、水平垂直方向の偏光を識別可能な測定器では、量子通信路上の、水平方向（０°）に偏光された光と垂直方向（９０°）に偏光された光とを正しく識別する。一方、斜め方向（４５°，１３５°）の偏光を識別可能な測定器では、量子通信路上の、４５°方向に偏光された光と１３５°方向に偏光された光とを正しく識別する。

このように、各測定器は、規定された方向に偏光された光については正しく認識できるが、たとえば、斜め方向に偏光された光を水平垂直方向（０°，９０°）の偏光を識別可能な測定器にて測定すると、水平方向と垂直方向に偏光された光をそれぞれ５０％の確率でランダムに識別する。すなわち、識別可能な偏光方向に対応していない測定器を用いた場合には、その測定結果を解析しても、偏光された方向を正しく識別することができない。

第１９図に示す従来の量子鍵配送では、上記不確定性（ランダム性）を利用して、盗聴者に知られずに送信者と受信者との間で鍵を共有する（たとえば、非特許文献１参照。）。なお、送信者および受信者は、量子通信路以外に公開通信路を使用することができる。

ここで、鍵の共有手順について説明する。まず、送信者は、乱数列（１，０の列：送信データ）を発生し、さらに送信コード（＋：水平垂直方向に偏光された光を識別可能な測定器に対応，×：斜め方向に偏光された光を識別可能な測定器に対応）をランダムに決定する。その乱数列と送信コードの組み合わせで、送信する光の偏光方向が自動的にきまる。ここでは、０と＋の組み合わせで水平方向に偏光された光を、１と＋の組み合わせで垂直方向に偏光された光を、０と×の組み合わせで４５°方向に偏光された光を、１と×の組み合わせで１３５°方向に偏光された光を、量子通信路にそれぞれ送信する（送信信号）。

つぎに、受信者は、受信コード（＋：水平垂直方向に偏光された光を識別可能な測定器，×：斜め方向に偏光された光を識別可能な測定器）をランダムに決定し、量子通信路上の光を測定する（受信信号）。そして、受信コードと受信信号の組み合わせによって受信データを得る。ここでは、受信データとして、水平方向に偏光された光と＋の組み合わせで０を、垂直方向に偏光された光と＋の組み合わせで１を、４５°方向に偏光された光と×の組み合わせで０を、１３５°方向に偏光された光と×の組み合わせで１を、それぞれ得る。

つぎに、受信者は、自身の測定が正しい測定器で行われたものかどうかを調べるために、受信コードを、公開通信路を介して送信者に対して送信する。受信コ

ードを受け取った送信者は、正しい測定器で行われたものかどうかを調べ、その結果を、公開通信路を介して受信者に対して返信する。

つぎに、受信者は、正しい測定器で受信した受信信号に対応する受信データだけを残し、その他を捨てる。この時点で、残された受信データは送信者と受信者との間で確実に共有できている。

つぎに、送信者と受信者は、それぞれの通信相手に対して、共有データから選択した所定数のデータを、公開通信路を経由して送信する。そして、受け取ったデータが自身の持つデータと一致しているかどうかを確認する。たとえば、確認したデータの中に一致しないデータが１つでもあれば、盗聴者がいるものと判断して共有データを捨て、再度、鍵の共有手順を最初からやり直す。一方、確認したデータがすべて一致した場合には、盗聴者がいないと判断し、確認に使用したデータを捨て、残った共有データを送信者と受信者の共有鍵とする。

一方、上記従来の量子鍵配送方法の応用として、たとえば、伝送路上におけるデータ誤りを訂正可能な量子鍵配送方法がある（たとえば、非特許文献２参照。）。

この方法では、送信者が、データ誤りを検出するために、送信データを複数のブロックに分割し、ブロック毎のパリティを公開通信路上に送信する。そして、受信者が、公開通信路を経由して受け取ったブロック毎のパリティと受信データにおける対応するブロックのパリティとを比較して、データ誤りをチェックする。このとき、異なるパリティがあった場合、受信者は、どのブロックのパリティが異なっているのかを示す情報を公開通信路上に返信する。そして、送信者は、該当するブロックをさらに前半部のブロックと後半部のブロックに分割し、たとえば、前半部のパリティを公開通信路上に返信する（二分探索）。以降、送信者と受信者は、上記二分探索を繰り返し実行することによりエラービットの位置を特定し、最終的に受信者がそのビットを訂正する。

さらに、送信者は、データに誤りがあるにもかかわらず、偶数個の誤りのために正しいと判定されたパリティがある場合を想定し、送信データをランダムに並

べ替えて（ランダム置換）複数のブロックに分割し、再度、上記二分探索による誤り訂正処理を行う。そして、ランダム置換によるこの誤り訂正処理を繰り返し実行することによって、すべてのデータ誤りを訂正する。

非特許文献１.

Bennett, C. H. and Brassard, G.: Quantum Cryptography: PublicKey Distribution and Coin Tossing, In Proceedings of IEEE Conference onComputers, System and Signal Processing, Bangalore, India, pp.175-179 (DEC.1984).

非特許文献２.

Brassard, G. and Salvail, L. 1993 Secret-Key Reconciliation by Public Discussion, In Advances in Cryptology - EUROCRYPT'93, Lecture Notes in Computer Science 765, 410-423.

しかしながら、上記第１９図に示す従来の量子鍵配送においては、誤り通信路を想定していないため、誤りがある場合には盗聴行為が存在したものとして上記共通データ（共通鍵）を捨てることとなり、伝送路によっては共通鍵の生成効率が非常に悪くなる、という問題があった。

また、上記伝送路上におけるデータ誤りを訂正可能な量子鍵配送方法においては、エラービットを特定するために膨大な回数のパリティのやりとりが発生し、さらに、ランダム置換による誤り訂正処理が所定回数にわたって行われるため、誤り訂正処理に多大な時間を費やすことになる、という問題があった。

本発明は、上記に鑑みてなされたものであって、極めて高い特性を持つ誤り訂正符号を用いて伝送路上におけるデータ誤りを訂正しつつ、高度に安全性の保証された共通鍵を生成することが可能な量子鍵配送方法を提供することを目的とする。

発明の開示

本発明にかかる量子鍵配送方法にあっては、量子通信路上の光子の測定結果と

して得られる確率情報付きの受信データの誤りを訂正することによって元の送信データを推定し、その推定結果を共有情報とする量子鍵配送方法であって、送信側および受信側の通信装置が、個別に、所望の範囲の符号化率で最適化された第１のパリティ検査行列（各装置で同一）を生成し、当該第１のパリティ検査行列から前記範囲内の特定の符号化率に対応した第２のパリティ検査行列（各装置で同一）を抽出する第１の検査行列生成ステップと、前記送信側の通信装置が、前記第２のパリティ検査行列と前記送信データに基づいて生成した第１の誤り訂正情報を、公開通信路を介して前記受信側の通信装置に通知する第１の誤り訂正情報通知ステップと、前記受信側の通信装置が、前記第１の誤り訂正情報に基づいて前記受信データの誤りを訂正する第１の誤り訂正ステップと、前記受信データの誤りを完全に訂正できなかった場合に、受信側および送信側の通信装置が、個別に、前回の誤り訂正情報が次の誤り訂正時における情報の一部となるように、前記第１のパリティ検査行列から前回の符号化率よりも低い符号化率に対応した第３のパリティ検査行列（各装置で同一）を抽出する第２の検査行列生成ステップと、前記送信側の通信装置が、前記第３のパリティ検査行列と前記送信データに基づいて生成した追加分の第２の誤り訂正情報を、公開通信路を介して前記受信側の通信装置に通知する第２の誤り訂正情報通知ステップと、前記受信側の通信装置が、前記第１および第２の誤り訂正情報に基づいて前記受信データの誤りを訂正する第２の誤り訂正ステップと、前記第１の誤り訂正ステップの処理で受信データの誤りを完全に訂正できた場合、または、前記第２の検査行列生成ステップ、前記第２の誤り訂正情報通知ステップ、前記第２の誤り訂正ステップの処理を繰り返し実行することにより誤りを完全に訂正できた場合、公開された誤り訂正情報量に応じて共有情報の一部を破棄し、その結果を暗号鍵とする暗号鍵生成ステップと、を含むことを特徴とする。

この発明によれば、確定的で特性が安定した「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用の検査行列を用いて受信データの誤りを訂正し、公開された誤り訂正情報に応じて共有情報の一部を捨てることとした。これにより、エラービットを特

定／訂正するための膨大な回数のパリティのやりとりがなくなり、誤り訂正情報を送信するだけで誤り訂正制御が行われるため、誤り訂正処理にかかる時間を大幅に短縮できる。また、公開された情報に応じて共有情報の一部を捨てているので、高度に安全性の保証された共通鍵を生成することができる。

また、本発明によれば、受信データの誤りを完全に訂正できるまで、符号化率を下げながら、所望の範囲の符号化率で最適化されたパリティ検査行列から特定符号化率に対応したパリティ検査行列を抽出し、さらに追加のシンドロームを生成し、この追加シンドロームを用いて誤り訂正処理を繰り返し実行することとした。これにより、通信路の雑音レベルを見積もるために生成した共有情報を破棄する必要がなくなるので、共有鍵の生成効率を大幅に向上させることができる。

図面の簡単な説明

第１図は、本発明にかかる量子暗号システムの構成を示す図であり、第２図は、実施の形態１の量子鍵配送の概要を示すフローチャートであり、第３図は、実施の形態１の量子鍵配送の概要を示すフローチャートであり、第４図は、パリティ検査行列$H_{R(1)}$の構成を示す図であり、第５図は、ユークリッド幾何符号に基づく「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」の構成法を示すフローチャートであり、第６図は、ユークリット幾何符号ＥＧ（２，2^2）のマトリクスを示す図であり、第７図は、並べ替え後のマトリクスを示す図であり、第８図は、最適化計算後の次数配分を示す図であり、第９図は、調整後の次数配分を示す図であり、第１０図は、パリティ検査行列$H_{R(3)}$を示す図であり、第１１図は、最適化計算の結果として得られた次数配分を示す図であり、第１２図は、追加行列$A_{R(2)}$を示す図であり、第１３図は、パリティ検査行列$H_{R(2)}$を示す図であり、第１４図は、追加行列$A_{R(1)}$の一具体例を示す図であり、第１５図は、パリティ検査行列$H_{R(1)}$の一具体例を示す図であり、第１６図は、送信側の通信装置が受信側の通信装置に対して送信するシンドロームS_Aを示す図であり、第１７図は、パリティ検査行列$H_{R(1)}$からパリティ検査行列$H_{R(L-1)}$を抽出する様子を示す図であり、第１８図は、追加シン

ドロームの生成方法を示す図であり、第１９図は、従来の偏光を利用した量子鍵配送の概要を示す図である。

発明を実施するための最良の形態

以下に、本発明にかかる量子鍵配送方法の実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。また、以下では、例として偏光を利用する量子鍵配送について説明するが、本発明は、たとえば、位相を利用するもの，周波数を利用するもの等にも適用可能であり、どのような量子状態を利用するかについては特に限定しない。

量子鍵配送は、盗聴者の計算能力によらず、安全性の保証された鍵配送方式であるが、たとえば、より効率よく共有鍵を生成するためには、伝送路を通ることによって発生するデータの誤りを取り除く必要がある。そこで、本実施の形態では、極めて高い特性をもつことが知られている低密度パリティ検査（ＬＤＰＣ：：Low-Density Parity-Check）符号を用いて誤り訂正を行う量子鍵配送について説明する。

第１図は、本発明にかかる量子暗号システム（送信側および受信側の通信装置）の構成を示す図である。この量子暗号システムは、情報m_aを送信する機能を備えた送信側の通信装置と、伝送路上で雑音等の影響を受けた情報m_a、すなわち情報m_bを受信する機能を備えた受信側の通信装置と、から構成される。

また、送信側の通信装置は、量子通信路を介して情報m_aを送信し、公開通信路を介してシンドロームS_Aを送信し、これらの送信情報に基づいて暗号鍵（受信側との共通鍵）を生成する暗号鍵生成部１と、暗号化部２１が暗号鍵に基づいて暗号化したデータを、送受信部２２が公開通信路を介してやりとりする通信部２と、を備え、受信側の通信装置は、量子通信路を介して情報m_bを受信し、公開通信路を介してシンドロームS_Aを受信し、これらの受信情報に基づいて暗号鍵（送信側との共通鍵）を生成する暗号鍵生成部３と、暗号化部４２が暗号鍵に基づいて暗号化したデータを、送受信部４１が公開通信路を介してやりとりする通信部４と、

を備える。

上記送信側の通信装置では、量子通信路上に送信する情報m_aとして、偏光フィルターを用いて所定の方向に偏光させた光を、受信側の通信装置に対して送信する。一方、受信側の通信装置では、水平垂直方向（０°，９０°）の偏光を識別可能な測定器と斜め方向（４５°，１３５°）の偏光を識別可能な測定器とを用いて、量子通信路上の、水平方向（０°）に偏光された光と垂直方向（９０°）に偏光された光と４５°方向に偏光された光と１３５°方向に偏光された光とを識別する。なお、各測定器は、規定された方向に偏光された光については正しく認識できるが、たとえば、斜め方向に偏光された光を水平垂直方向（０°，９０°）の偏光を識別可能な測定器にて測定すると、水平方向と垂直方向に偏光された光をそれぞれ５０％の確率でランダムに識別する。すなわち、識別可能な偏光方向に対応していない測定器を用いた場合には、その測定結果を解析しても、偏光された方向を正しく識別することができない。

以下、上記量子暗号システムにおける各通信装置の動作、すなわち、本実施の形態における量子鍵配送について詳細に説明する。第２図および第３図は、本実施の形態の量子鍵配送の概要を示すフローチャートであり、詳細には、第２図は送信側の通信装置の処理を示し、第３図は受信側の通信装置の処理を示す。

まず、上記送信側の通信装置および受信側の通信装置では、パリティ検査行列生成部１０，３０が、特定の線形符号のパリティ検査行列Ｈを求める（ステップＳ１）。なお、符号化率は「０＜Ｒ（１）＜Ｒ（２）＜…＜Ｒ（ｍａｘ）＝１（Ｒ（ｍａｘ）は無符号化を表す）」であり、ここでは、一例として、符号化率が限りなく”０”に近いパリティ検査行列$H_{R(L)}$を求めることとする。

そして、上記パリティ検査行列$H_{R(L)}$から任意の符号化率Ｒ（Ｌ）＝（ｎ－ｋ）／ｎのパリティ検査行列$H_{R(L)}$（ｎ×ｋ行列）を抽出し、このパリティ検査行列$H_{R(L)}$から「$H_{R(L)}G_{R(L)}=0$」を満たす生成行列$G_{R(L)}$（（ｎ－ｋ）×ｎ行列）を求め、さらに、$G_{R(L)}^{-1}\cdot G_{R(L)}=I$（単位行列）となる$G_{R(L)}$の逆行列$G_{R(L)}^{-1}$（ｎ×（ｎ－ｋ）行列）を求める（ステップＳ１，ステップＳ１１）。ここでは、上記任意の

符号化率Ｒ（Ｌ）を、説明の便宜上、Ｒ（Ｌ）＝０．６とする。

本実施の形態では、上記特定の線形符号として、シャノン限界に極めて近い優れた特性をもつＬＤＰＣ符号を用いた場合の量子鍵配送について説明する。なお、上記特定の線形符号としては、ターボ符号等の他の線形符号を用いることとしてもよい。また、たとえば、後述する誤り訂正情報（シンドローム）が適当な行列Ｈと送信データm_A（情報m_aの一部）の積Hm_Aで表される誤り訂正プロトコル（たとえば、従来技術にて説明した「伝送路上におけるデータ誤りを訂正可能な量子鍵配送」に相当する誤り訂正プロトコル）であれば、すなわち、誤り訂正情報と送信データm_Aの線形性が確保されるのであれば、その行列Ｈをパリティ検査行列として用いることとしてもよい。

ここで、上記パリティ検査行列生成部１０におけるＬＤＰＣ符号の構成法（ステップＳ１の処理に相当）について説明する。

なお、ここでは、ＬＤＰＣ符号$C_{R(l)}$のパリティ検査行列を$H_{R(l)}$とする。また、符号化率Ｒ（ｌ），ｌ＝１，２，…，ｍａｘは、「０＜Ｒ（１）＜Ｒ（２）＜…＜Ｒ（ｍａｘ）＝１」である。Ｒ（ｍａｘ）は無符号化を表す。

また、パリティ検査行列$H_{R(l)}$は、パリティ検査行列$H_{R(l+1)}$と追加のパリティ検査行列$A_{R(l)}$を用いて、下記（１）式のように定義することができる。第４図は、（１）式の概要を示す図である。

$$H_{R(l)} = \left[\frac{H_{R(l+1)}}{A_{R(l)}} \right] \qquad \cdots (1)$$

ただし、パリティ検査行列$H_{R(l)}$とパリティ検査行列$H_{R(l+1)}$はともにフルランクである。

また、本実施の形態では、ガウス近似法によりパリティ検査行列$H_{R(l)}$，ｌ＝１，２，…，ｍａｘの次数配分を最適化する。すなわち、下記（２）式を最小化するようなパリティ検査行列$H_{R(l)}$の次数配分を求める。

$$\sum_{l=1}^{max} GAP_{R(l)} \quad \cdots (2)$$

ただし、$GAP_{R(l)}$は、ガウス近似法で推定するパリティ検査行列$H_{R(l)}$の反復しきい値のＳＮＲとシャノン限界との差をｄＢで表現したものである。

上記（２）式を最小化するようなパリティ検査行列$H_{R(l)}$の次数配分の求め方としては、たとえば、下記（３）式、すなわち、ガウスノイズσ_n（Ｒ（１））を最大とするλ（ｘ，Ｒ（１）），ρ（ｘ，Ｒ（１））を探索する計算を行う。下記（３）式を計算する場合の拘束条件を下記（４）式，（５）式，（６）式，（７）式に示す。

$$\sum_{l=1}^{max} \sigma_n(R(l)) \quad \cdots (3)$$

$$\frac{\int_0^1 \rho(x,R(l))}{\int_0^1 \lambda(x,R(l))} = 1 - R(l)$$

$$\lambda(x,R(l)) = \lambda_1(R(l)) + \lambda_2(R(l))x^1 + \Lambda + \lambda_{dv(max,R(l))}(R(l))x^{dv(max,R(l))-1}$$

$$\rho(x,R(l)) = \rho_1(R(l)) + \rho_2(R(l))x^1 + \Lambda + \rho_{dc(max,R(l))}(R(l))x^{dc(max,R(l))-1} \quad \cdots (4)$$

$$\lambda(x,R(l)) = 1$$

$$\rho(x,R(l)) = 1 \quad \cdots (5)$$

$$r > \sum_{i=2}^{dv(max,R(l))} \lambda_i(R(l))\phi\left(s+(i-1)\sum_{j=2}^{dc(max,R(l))}\rho_j(R(l))\phi^{-1}\left(1-(1-r)^{j-1}\right)\right)$$

$$\forall r \in (0,\phi(s))$$

$$0 \le \lambda_i(R(l)) \le 1, \quad \lambda_i(R(l)) \in R$$

$$0 \le \rho_i(R(l)) \le 1, \quad \rho_i(R(l)) \in R$$

$$\phi(x) = \begin{cases} 1-\dfrac{1}{\sqrt{4\pi x}}\int_R \tanh\dfrac{u}{2}\cdot e^{\frac{(u-x)^2}{4x}}du, & \text{if } x>0 \\ 1, & \text{if } x \le 0 \end{cases} \quad \cdots (6)$$

$$\lambda_x(R(l)) \le \frac{\left(\sum_{i=2}^{x} n_v(i,R(l+1))\times i\right)-\left(\sum_{j=2}^{x-1} n_v(j,R(l))\times j\right)}{H_{R(l)}\text{の"1"の総数}} \quad \cdots (7)$$

ただし、λ_i（R（l））はパリティ検査行列$H_{R(l)}$の次数ｉの列の比率を表し、ρ_i（R（l））はパリティ検査行列$H_{R(l)}$の次数ｉの行の比率を表す。また、ｄｖ（ｍａｘ，R（l））はパリティ検査行列$H_{R(l)}$の列の最大次数を表し、ｄｃ（ｍａｘ，R（l））はパリティ検査行列$H_{R(l)}$の行の最大次数を表す。また、λ（ｘ，R（l））はパリティ検査行列$H_{R(l)}$の列の次数分布の生成関数であり、ρ（ｘ，R（l））はパリティ検査行列$H_{R(l)}$の行の次数分布の生成関数である。また、n_v（ｉ，R（l））はパリティ検査行列$H_{R(l)}$の次数ｉの列数を表し、n_c（ｉ，R（l））はパリティ検査行列$H_{R(l)}$の次数ｉの行数を表す。

以下に、上記ステップＳ１にてパリティ検査行列$H_{R(l)}$を求める処理の一例として、パリティ検査行列$H_{R(3)}$，パリティ検査行列$H_{R(2)}$，パリティ検査行列$H_{R(1)}$を順に求める場合の処理について具体的に説明する。第５図は、ユークリッド幾何符号に基づく「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」の構成法を示すフローチャートである。なお、パリティ検査行列生成部３０については、パリティ検査行列生

成部１０と同様に動作するのでその説明を省略する。また、本実施の形態における検査行列生成処理は、たとえば、設定されるパラメータに応じてパリティ検査行列生成部１０で実行する構成としてもよいし、通信装置外部の他の制御装置（計算機等）で実行することとしてもよい。本実施の形態における検査行列生成処理が通信装置外部で実行される場合は、生成済みの検査行列が通信装置に格納される。以降の実施の形態では、パリティ検査行列生成部１０で上記処理を実行する場合について説明する。

まず、パリティ検査行列生成部１０では、符号長および符号化率を決定する（第５図、ステップＳ２１）。ここでは、たとえば、符号長をｎ＝５０００とし、符号化率をＲ（３）＝０．６，Ｒ（２）＝０．４，Ｒ（１）＝０．０とする。

つぎに、パリティ検査行列生成部１０では、ユークリッド幾何符号ＥＧ（２，2^s）を選択し、さらに、「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用の検査行列のベースとなる基本行列Ａ（ｓ＝５，Ｒ（３）），Ａ（ｓ＝５，Ｒ（２）），Ａ（ｓ＝５，Ｒ（１））を生成する（ステップＳ２２）。たとえば、ｓ＝５とした場合、ユークリッド幾何符号ＥＧ（２，2^5）の一行目の重み分布（”１”の列番号）は、下記のようになる。

{1 32 114 136 149 223 260 382 402 438 467 507 574 579 588 622 634 637 638 676 717 728 790 851 861 879 947 954 971 977 979 998}

ＬＤＰＣ符号を用いた符号化／復号においては、一般的に、２部グラフ上に「サイクル４」および「サイクル６」が少ないほど良好な特性を得ることができる。そこで、本実施の形態では、「サイクル４」や「サイクル６」といった少ないサイクルを抑制するように、ユークリッド幾何符号ＥＧ（２，2^5）の１行目の重み分布から適当に”１”を間引きする。間引き後の重み分布は、たとえば、下記のようになる。

{1 32 114 136 149 223 260 402 438 467 507 574 588 634 638 717 728 790 861 947 971 979}

そして、間引き後の重み分布に基づいて、各基本行列の一行目の重み分布を決

定し（個別に上記”１”の位置を割り当てる）、さらに、その重み分布を巡回シフトすることにより、１０２３行×１０２３列の基本行列Ａ（ｓ＝５，Ｒ（３）），Ａ（ｓ＝５，Ｒ（２）），Ａ（ｓ＝５，Ｒ（１））を生成する。本実施の形態では、各基本行列の一行目の重み分布を、たとえば、下記のように決定する。

Ａ（ｓ＝５，Ｒ（３））＝｛1 32 114 149 260 402 467 507 574 634 717 728 790 861 979｝

Ａ（ｓ＝５，Ｒ（２））＝｛223 438 947｝

Ａ（ｓ＝５，Ｒ（１））＝｛136 588 638 971｝

これにより、パリティ検査行列$H_{R(3)}$の列の最大次数がｄｖ（ｍａｘ，Ｒ（３））＝１５となり、パリティ検査行列$H_{R(2)}$の列の最大次数がｄｖ（ｍａｘ，Ｒ（２））＝３となり、パリティ検査行列$H_{R(1)}$の列の最大次数がｄｖ（ｍａｘ，Ｒ（１））＝４となる。また、パリティ検査行列$H_{R(3)}$の行の最大次数がｄｃ（ｍａｘ，Ｒ（３））＝１５となり、パリティ検査行列$H_{R(2)}$の行の最大次数がｄｃ（ｍａｘ，Ｒ（２））＝３となり、パリティ検査行列$H_{R(1)}$の行の最大次数がｄｃ（ｍａｘ，Ｒ（１））＝４となる。

つぎに、パリティ検査行列生成部１０では、上記各基本行列を、列内の”１”の位置が列中のできるだけ上部にくるように、以下の手順で並べ替えを行う（ステップＳ２３）。この並べ替え手順を一般的に表現すると、下記（８）式のように表現できる。

$$h_k(X) \in GF(2)[X]/X^{(2^{2s}-1)}$$

$$k = \left\{1,2,\ldots,2^2\cdot(2^{2s}-1)\right\}$$

$$\begin{bmatrix} h_{i+0}(X) \\ h_{i+1}(X) \\ h_{i+2}(X) \\ M \\ M \end{bmatrix} = \begin{bmatrix} X^{-(w1-1)} \\ X^{-(w2-1)} \\ X^{-(w3-1)} \\ M \\ M \end{bmatrix} \cdot \left[\left(X^{(w1-1)} + X^{(w2-1)} + \Lambda\right) \cdot X^{(i-1)}\right] \quad \cdots (8)$$

なお、ｉ＝１～$2^{2s}-1$とする。また、（８）式の多項式（$X^{(w1-1)}+X^{(w2-1)}+\cdots$

）は、各基本行列の最初の行を表現した式である。たとえば、基本行列の重みの位置が｛1 7 9 … 40｝の場合は、$1+X^{(7-1)}+X^{(9-1)}+\cdots X^{(40-1)}$となる。

そして、上記（8）式において、i＝1～$2^{2s}-1$，j＝1～i－1までの間に、$h_i(X)=h_j(X)$が存在する場合は、$h_i(X)$を削除する。この並べ替え処理により、後述する行の削除処理（短縮処理）を行う場合に、できるだけ重みの大きい列を残すことができ、かつ列内の重みのバリエーションをできるだけ少なくすることができる。

具体例として、たとえば、ユークリット幾何符号ＥＧ（2，2^2）を基本行列とした場合、上記並べ替え手順を実施すると、第６図に示すマトリクスが第７図に示すマトリクスのように並べ替えられる。第６図は、ユークリット幾何符号ＥＧ（2，2^2）のマトリクスを示す図（空白は０を表す）であり、第７図は、並べ替え後のマトリクスを示す図である。

つぎに、パリティ検査行列生成部１０では、上記で決定した符号長ｎ＝５０００，符号化率Ｒ（３）＝０．６，並べ替え後の基本行列Ａ（ｓ＝５，Ｒ（３））を用いて、２０００行×５０００列のパリティ検査行列$H_{R(3)}$を求める処理（最適化計算）を実行する（ステップＳ２４）。

ここでは、まず、ガウスノイズσ_n（Ｒ（３））を最大とする生成関数λ（ｘ，Ｒ（３）），ρ（ｘ，Ｒ（３））を探索する。この場合、上記（４）式，（５）式，（６）式が拘束条件となる。第８図は、最適化計算後の次数配分を示す図である。

また、パリティ検査行列生成部１０では、基本行列Ａ（ｓ＝５，Ｒ（３））と鍵長ｎ＝５０００と符号化率Ｒ（３）＝０．６に基づいて、短縮行列を求める。たとえば、$\mu_i \in Z$（正の整数）を、基本行列Ａ（ｓ，Ｒ（１））の１行から分割された次数ｉの行数とすると、行の分割数は、下記（９）式となる。

$$\sum_{i=1}^{dc(max,R(1))} \rho_i(R(1)) \times \mu_i = 1$$

$$\text{行の分割数} = \sum_{i=1}^{dc(max,R(1))} \mu_i \qquad \cdots (9)$$

第８図の例では、$7\mu_7/15+8\mu_8/15=1$（ただし、$\mu_7=1$，$\mu_8=1$）となり、行の分割数は、「１＋１＝２」となる。

そして、短縮行列の行数は、下記（１０）式となる。

短縮行列の行数＝ｎ×（１－Ｒ（３））／行の分割数

＝５０００×（１－０．６）／２＝１０００　…（１０）

すなわち、ここでは、１０２３行の基本行列Ａ（ｓ＝５，Ｒ（３））の最下位から２３行を削除して、１０００行の短縮行列Ａ´（ｓ＝５，Ｒ（３））を生成する。

その後、パリティ検査行列生成部１０では、第８図に示す行の次数比率ρ_i（Ｒ（３））と行の次数ｉを固定した状態で、上記短縮行列Ａ´（ｓ＝５，Ｒ（３））を用いて構成可能な、パリティ検査行列$H_{R(3)}$の次数ｉ＝２，３，４の列数n_v（ｉ，Ｒ（３））と、パリティ検査行列$H_{R(3)}$の次数ｉ＝７，８の行数n_c（ｉ，Ｒ（３））と、を求める。ここでは、分割後の行列の列が５０００列になるように、列の次数比率λ_i（Ｒ（３））を調整する。第９図は、調整後の次数配分を示す図である。

その後、第９図に示す次数分布に基づいて、短縮行列Ａ´（ｓ＝５，Ｒ（３））の行と列を分割し、その結果を２０００行×５０００列のパリティ検査行列$H_{R(3)}$´とする。さらに、分割後のパリティ検査行列$H_{R(3)}$´の列の重みが昇順になるように列を並べ替えて、並べ替え後の行列をパリティ検査行列$H_{R(3)}$とする。第１０図は、パリティ検査行列$H_{R(3)}$を示す図である。ここでは、重み”７”の行が１０００行、重み”８”の行が１０００行、重み”２”の列が２７９列、重み”３

”の列が４４４２列、重み” ４”の列が２７９列となる。

なお、本実施の形態における短縮行列の分割処理（後述する分割処理も含む）は、規則的に分割するのではなく、各行または各列から「１」をランダムに抽出することにより行う（ランダム分割）。なお、この抽出処理は、ランダム性が保持されるのであればどのような方法を用いてもよい。

つぎに、パリティ検査行列生成部１０では、上記で決定した符号長ｎ＝５０００，符号化率Ｒ（２）＝０．４，並べ替え後の基本行列Ａ（ｓ＝５，Ｒ（２）），パリティ検査行列$H_{R(3)}$を用いて、下記（１１）式に示すパリティ検査行列$H_{R(2)}$および追加行列$A_{R(2)}$を求める処理（最適化計算）を実行する（ステップＳ２５）。ここでは、上記パリティ検査行列$H_{R(3)}$を求める処理と異なる処理についてのみ説明する。

$$H_{R(2)} = \left[\frac{H_{R(3)}}{A_{R(2)}} \right] \qquad \cdots (11)$$

まず、ガウスノイズσ_n（Ｒ（２））を最大とする生成関数λ（ｘ，Ｒ（２））ρ（ｘ，Ｒ（２））を探索する。なお、この最適化計算では、上記（４）式，（５）式，（６）式に加えて、（７）式が拘束条件となる。具体的には、（７）式に基づいて生成された（１２）式を満たすことが拘束条件となる。

$$\lambda_x(R(l-1)) \le \frac{\left(\sum_{i=2}^{x} n_v(i, R(l)) \times i\right) - \left(\sum_{j=2}^{x-1} n_v(j, R(l-1)) \times j\right)}{H_{R(l-1)}\text{の"1"の総数}} \qquad \cdots (12)$$

したがって、たとえば、パリティ検査行列$H_{R(2)}$における次数２，次数３，次数４の拘束条件は、それぞれ（１３）式，（１４）式，（１５）式となる。

$$\lambda_2 \le \frac{n_v(2,R(1))\times 2}{1000\times 15+1000\times 3}$$
$$= \frac{279\times 2}{18000} \quad \cdots (13)$$
$$= 0.031$$

$$\lambda_3 \le \frac{n_v(3,R(1))\times 3+n_v(2,R(1))\times 2-n_v(2,R(1-1))\times 2}{1000\times 15+1000\times 3}$$
$$= \frac{4686\times 3+279\times 2-n_v(2,R(1-1))\times 2}{6\times 5000\times 0.6}$$
$$= 0.812-\frac{n_v(2,R(1-1))}{9000} \quad \cdots (14)$$

$$\lambda_4 \le \frac{n_v(4,R(1))\times 4+n_v(3,R(1))\times 3+n_v(2,R(1))\times 2-\left(n_v(3,R(1-1))\times 3+n_v(2,R(1-1))\times 2\right)}{1000\times 15+1000\times 3}$$
$$= \frac{96\times 4+4686\times 3+279\times 2-\left(n_v(3,R(1-1))\times 3+n_v(2,R(1-1))\times 2\right)}{18000}$$
$$= 0.833-\frac{\left(n_v(3,R(1-1))\times 3+n_v(2,R(1-1))\times 2\right)}{18000} \quad \cdots (15)$$

さらに、パリティ検査行列$H_{R(2)}$の列の最大次数が下記（１６）式を満たすことも拘束条件となる。

$H_{R(2)}$の列の最大次数＝$H_{R(3)}$の列の最大次数＋Ａ（ｓ＝５，Ｒ（２））の要素数 … （１６）

第１１図は、上記最適化計算の結果として得られた次数配分を示す図である。

一方で、パリティ検査行列生成部１０では、基本行列Ａ（ｓ＝５，Ｒ（２））の要素数と鍵長ｎ＝５０００と符号化率Ｒ（２）＝０．４を用いて、上記（９）式、上記（１０）式と同様の処理で短縮行列Ａ´（ｓ＝５，Ｒ（２））を求める。

第１１図の例では、$3\mu_3/18+7\mu_7/18+8\mu_8/18=1$（ただし、$\mu_3$

＝１，μ_7＝１，μ_8＝１）となり、行の分割数は、「１＋１＋１＝３」となる。

すなわち、ここでも、１０２３行の基本行列Ａ（ｓ＝５，Ｒ（２））の最下位から２３行を削除して、１０００行の短縮行列Ａ´（ｓ＝５，Ｒ（２））を生成する。

その後、第１１図に示す次数分布に基づいて、短縮行列Ａ´（ｓ＝５，Ｒ（２））の列を分割し、その結果を１０００行×５０００列の仮追加行列$A_{R(2)}$´とする。さらに、分割後の仮追加行列$A_{R(2)}$´の列の重みが昇順になるように列を並べ替えて、並べ替え後の行列を正式な追加行列$A_{R(2)}$とする。第１２図は、追加行列$A_{R(2)}$を示す図である。ここでは、重み”３”の行が１０００行、重み”１”の列が１５０列、重み”２”の列が６列、重み”３”の列が９４６列となる。また、第１３図は、パリティ検査行列$H_{R(2)}$を示す図である。

最後に、パリティ検査行列生成部１０では、上記で決定した符号長ｎ＝５０００，符号化率Ｒ（２）＝０．０，並べ替え後の基本行列Ａ（ｓ＝５，Ｒ（１）），パリティ検査行列$H_{R(2)}$を用いて、下記（１７）式に示すパリティ検査行列$H_{R(1)}$および追加行列$A_{R(1)}$を求める処理（最適化計算）を実行する（ステップＳ２６）。この処理は、上記パリティ検査行列$H_{R(2)}$を求める処理と同様の手順で行う。

$$H_{R(1)} = \left[\frac{H_{R(2)}}{A_{R(1)}} \right] \qquad \cdots (17)$$

その後、上記計算結果として得られる次数分布に基づいて、短縮行列Ａ´（ｓ＝５，Ｒ（１））の行および列を分割し、その結果を２０００行×５０００列の仮追加行列$A_{R(1)}$´とする。さらに、分割後の仮追加行列$A_{R(1)}$´の列の重みが昇順になるように列を並べ替えて、並べ替え後の行列を正式な追加行列$A_{R(1)}$とする。第１４図は、追加行列$A_{R(1)}$の一具体例を示す図である。また、第１５図は、パリティ検査行列$H_{R(1)}$の一具体例を示す図である。

このように、本実施の形態では、上記ステップＳ２１～Ｓ２６を実行することによって、確定的で特性が安定した「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用の

検査行列$H_{R(3)}$，$H_{R(2)}$，$H_{R(1)}$を生成することができる。

なお、本実施の形態においては、基本となる符号（基本行列）にユークリッド幾何符号を用いることとしたが、これに限らず、「行と列の重みが一定」かつ「２部グラフ上のサイクル数が６以上」という条件を満たす行列であれば、ユークリッド幾何符号以外（Ｃａｙｌｅｙグラフによる基本行列やＲａｍａｎｕｊａｎグラフによる基本行列等）の行列を用いることとしてもよい。

また、本実施の形態では、最終的に、符号化率が限りなく”０”に近いパリティ検査行列$H_{R(1)}$を生成することとしたが、これに限らず、通信環境によって必要に応じた大きさ（$H_{R(2)}$，$H_{R(3)}$，$H_{R(4)}$等）のパリティ検査行列を予め生成しておくこととしてもよい。また、本実施の形態では、３段構成のパリティ検査行列を想定したが、良好な特性が得られるのであれば、何段構成であってもかまわない。

上記のように、パリティ検査行列$H_{R(1)}$，生成行列$G_{R(L)}$，$G^{-1}{}_{R(L)}$を生成後、つぎに、送信側の通信装置では、乱数発生部１１が、乱数列m_a（１，０の列：送信データ）を発生し、さらに送信コード（＋：水平垂直方向に偏光された光を識別可能な測定器に対応したコード，×：斜め方向に偏光された光を識別可能な測定器に対応したコード）をランダムに決定する（第２図、ステップＳ２）。一方、受信側の装置では、乱数発生部３１が、受信コード（＋：水平垂直方向に偏光された光を識別可能な測定器に対応したコード，×：斜め方向に偏光された光を識別可能な測定器に対応したコード）をランダムに決定する（第３図、ステップＳ１２）。

つぎに、送信側の通信装置では、光子生成部１２が、上記乱数列m_aと送信コードの組み合わせで自動的に決まる偏光方向で光子を送信する（ステップＳ３）。たとえば、０と＋の組み合わせで水平方向に偏光された光を、１と＋の組み合わせで垂直方向に偏光された光を、０と×の組み合わせで４５°方向に偏光された光を、１と×の組み合わせで１３５°方向に偏光された光を、量子通信路にそれぞれ送信する（送信信号）。

光子生成部１２の光信号を受け取った受信側の通信装置の光子受信部３２では、

量子通信路上の光を測定する（受信信号）。そして、受信コードと受信信号の組み合わせによって自動的に決まる受信データm_bを得る（ステップＳ１３）。ここでは、受信データm_bとして、水平方向に偏光された光と＋の組み合わせで０を、垂直方向に偏光された光と＋の組み合わせで１を、４５°方向に偏光された光と×の組み合わせで０を、１３５°方向に偏光された光と×の組み合わせで０を、それぞれ得る。なお、受信データm_bは、確率情報付きの硬判定値とする。

つぎに、受信側の通信装置では、上記測定が正しい測定器で行われたものかどうかを調べるために、乱数発生部３１が、受信コードを、公開通信路を介して送信側の通信装置に対して送信する（ステップＳ１３）。受信コードを受け取った送信側の通信装置では、上記測定が正しい測定器で行われたものかどうかを調べ、その結果を、公開通信路を介して受信側の通信装置に対して送信する（ステップＳ３）。そして、受信側の通信装置および送信側の通信装置では、正しい測定器で受信した受信信号に対応するデータだけを残し、その他を捨てる（ステップＳ３，Ｓ１３）。その後、残ったデータをメモリ等に保存し、その先頭から順にｎビットを読み出し、これを、正式な送信データm_Aと受信データm_B（m_Bは伝送路上で雑音等の影響を受けたm_A：$m_B=m_A+e$（雑音等））とする。すなわち、ここでは、必要に応じてつぎのｎビットを読み出して、送信データm_Aと受信データm_Bを生成する。本実施の形態では、残ったデータのビット位置が、送信側の通信装置と受信側の通信装置との間で共有できている。なお、m_Bは、上記m_b同様、確率情報付きの硬判定値である。

つぎに、送信側の通信装置では、シンドローム生成部１４が、パリティ検査行列$H_{R(L)}$（ｎ×ｋの行列）と送信データm_Aを用いてm_Aのシンドローム$S_A=H_{R(L)}m_A$を計算し、その結果を、公開通信路通信部１３，公開通信路を介して受信側の通信装置に通知する（ステップＳ４）。この段階で、m_AのシンドロームS_A（ｋビット分の情報）は盗聴者に知られる可能性がある。第１６図は、送信側の通信装置が受信側の通信装置に対して送信するシンドロームS_Aを示す図である。一方、受信側の通信装置では、公開通信路通信部３４にてm_AのシンドロームS_Aを受

信し、それをシンドローム復号部３３に通知する（ステップＳ１４）。

つぎに、シンドローム復号部３３では、既知のシンドローム復号法を用いて、雑音等による確率情報付きの硬判定値m_Bの誤りを訂正することによって元の送信データm_Aを推定する（ステップＳ１５）。本実施の形態では、たとえば、「$S_A = H_{R(L)} m_C$」を満たすm_Cを確率情報付きの硬判定値m_Bから推定し、その推定結果m_Cを共有情報m_Aとする。なお、本実施の形態においては、受信データm_Bおよびm_bを確率情報付きの硬判定値としたが、これに限らず、たとえば、軟判定値とした場合においても適用可能であり、どのような受信データを利用するかについては特に規定しない。

そして、ステップＳ１５の処理によって硬判定値m_Bの誤りを完全に訂正できた場合（ステップＳ１５，ＯＫ）、受信側の通信装置では、共有鍵生成部３５が、公開された誤り訂正情報（盗聴された可能性のある上記ｋビット分の情報：S_A）に応じて共有情報m_Aの一部を捨てて、ｎ－ｋビット分の情報量を備えた暗号鍵ｒを生成する（ステップＳ１６）。すなわち、共有鍵生成部３５では、先に計算しておいた$G_{R(L)}^{-1}$（ｎ×（ｎ－ｋ）の行列）を用いて下記（１８）式により暗号鍵ｒを生成する。受信側の通信装置は、この暗号鍵ｒを送信側の通信装置との共有鍵とする。

$$r = G_{R(L)}^{-1} m_A \qquad \cdots (18)$$

また、送信側の通信装置においては、ステップＳ１５の処理によって硬判定値m_Bの誤りが完全に訂正され、新たなシンドローム要求がない場合（ステップＳ５，Ｙｅｓ）、共有鍵生成部１５が、公開された誤り訂正情報（盗聴された可能性のある上記ｋビット分の情報：S_A）に応じて共有情報m_Aの一部を捨てて、ｎ－ｋビット分の情報量を備えた暗号鍵ｒを生成する（ステップＳ６）。すなわち、共有鍵生成部１５でも、先に計算しておいた$G_{R(L)}^{-1}$（ｎ×（ｎ－ｋ）の行列）を用いて上記（１８）式により暗号鍵ｒを生成する（ステップＳ６）。送信側の通信装置は、この暗号鍵ｒを受信側の通信装置との共有鍵とする。

なお、本実施の形態においては、さらに、正則なランダム行列Ｒを用いて上記

共有鍵を並べ替える構成としてもよい。これにより、秘匿性を増強させることができる。具体的には、まず、送信側の通信装置が、正則なランダム行列Ｒ（（ｎ－ｋ）×（ｎ－ｋ）の行列）を生成し、さらに、当該Ｒを、公開通信路を介して受信側の通信装置に通知する。なお、この処理は、受信側の通信装置で行うこととしてもよい。その後、送信側および受信側の通信装置が、先に計算しておいた$G_{R(L)}^{-1}$（ｎ×（ｎ－ｋ）の行列）とランダム行列Ｒを用いて下記（１９）式により暗号鍵ｒを生成する。

$$r = R G_{R(L)}^{-1} m_A \quad \cdots (19)$$

一方、ステップＳ１５の処理によって硬判定値m_Bの誤りを完全に訂正できなかった場合（ステップＳ１５，ＮＧ）、受信側の通信装置のシンドローム復号部３３では、公開通信路通信部３４，公開通信路を介して送信側の通信装置にシンドローム要求を通知する（ステップＳ１７）。そして、パリティ検査行列生成部３０では、上記パリティ検査行列$H_{R(1)}$から、符号化率Ｒ（Ｌ－１）＝（ｎ－ｋ－ｔ）／ｎのパリティ検査行列$H_{R(L-1)}$（ｎ×（ｋ＋ｔ）行列）を抽出し（符号化率を下げる）、このパリティ検査行列$H_{R(L-1)}$から「$H_{R(L-1)} G_{R(L-1)} = 0$」を満たす生成行列$G_{R(L-1)}$を生成し、さらに、$G_{R(L-1)}^{-1} \cdot G_{R(L-1)} = I$（単位行列）となる$G_{R(L-1)}$の逆行列$G_{R(L-1)}^{-1}$を生成する（ステップＳ１８）。

第１７図は、パリティ検査行列$H_{R(1)}$からパリティ検査行列$H_{R(L-1)}$を抽出する様子を示す図である。本実施の形態では、図示のとおり、符号化率に応じた大きさのパリティ検査行列を、予め生成しておいたパリティ検査行列$H_{R(1)}$から切り出すことによって、追加シンドローム送信時のパリティ検査行列を生成する。すなわち、符号化率に応じた最適化計算（ガウス近似法）をその都度実行することなく、符号化率に応じた大きさのパリティ検査行列を容易に生成できる。

なお、符号化率の下げ幅は、システムの要求条件に依存する。たとえば、符号化率の下げ幅を小さくした場合には、誤り訂正処理の回数を増加させてしまう可能性があるが、一方で、鍵の生成率が向上する。また、符号化率の下げ幅を大きくした場合には、誤り訂正処理の回数を低減できるが、一方で、鍵の生成率が低

下する。

つぎに、シンドローム要求を受け取った（ステップＳ５，Ｎｏ）送信側の通信装置のパリティ検査行列生成部１０においても、同様に、上記パリティ検査行列$H_{R(1)}$から、符号化率Ｒ（Ｌ－１）＝（ｎ－ｋ－ｔ）／ｎのパリティ検査行列$H_{R(L-1)}$（ｎ×（ｋ＋ｔ）行列）を抽出し、このパリティ検査行列$H_{R(L-1)}$から「$H_{R(L-1)}G_{R(L-1)}=0$」を満たす生成行列$G_{R(L-1)}$を生成し、さらに、$G_{R(L-1)}^{-1}\cdot G_{R(L-1)}=I$（単位行列）となる$G_{R(L-1)}$の逆行列$G_{R(L-1)}^{-1}$を生成する（ステップＳ７）。

つぎに、送信側の通信装置では、シンドローム生成部１４が、パリティ検査行列$H_{R(L-1)}$（ｎ×（ｋ＋ｔ）の行列）と送信データm_Aを用いてｔ行分のシンドロームS_A'を計算し、その結果を、公開通信路通信部１３，公開通信路を介して受信側の通信装置に通知する（ステップＳ８）。第１８図は、追加シンドロームの生成方法を示す図である。なお、この段階で、シンドロームS_A'（ｔビット分の情報）は盗聴者に知られる可能性がある。そして、受信側の通信装置では、公開通信路通信部３４にてｔ行分のシンドロームS_A'を受信し、それをシンドローム復号部３３に通知する（ステップＳ１９）。

つぎに、シンドローム復号部３３では、上記既知のシンドローム復号法を用いて、確率情報付きの硬判定値m_Bの誤りを訂正し、再度、元の送信データm_Aを推定する（ステップＳ１５）。

以降、本実施の形態の受信側の通信装置においては、ステップＳ１５の処理により硬判定値m_Bの誤りを完全に訂正できるまで、符号化率を下げながらパリティ検査行列$H_{R(1)}$から所望のパリティ検査行列を抽出してステップＳ１７～Ｓ１９の処理を繰り返し実行し、誤りを完全に訂正できた段階で、共有鍵生成部３５が、公開された誤り訂正情報（たとえば、盗聴された可能性のある上記ｋ＋ｔビット分の情報：S_A+S_A'（第１８図参照））に応じて共有情報m_Aの一部を捨てて、たとえば、ｎ－ｋ－ｔ，ｎ－ｋ－２ｔ，ｎ－ｋ－３ｔ，…ビット分の情報量を備えた暗号鍵ｒを生成する（ステップＳ１６）。受信側の通信装置は、この暗号鍵ｒを送信側の通信装置との共有鍵とする。

また、本実施の形態の送信側の通信装置においては、新たなシンドローム要求が通知されなくなるまで、符号化率を下げながらパリティ検査行列$H_{R(1)}$から所望のパリティ検査行列を抽出してステップＳ７，Ｓ８の処理を繰り返し実行し、新たなシンドローム要求が通知されなくなった段階で、共有鍵生成部１５が、公開された誤り訂正情報（たとえば、盗聴された可能性のある上記ｋ＋ｔビット分の情報：S_A+S_A'（図７参照））に応じて共有情報m_Aの一部を捨てて、たとえば、ｎ－ｋ－ｔ，ｎ－ｋ－２ｔ，ｎ－ｋ－３ｔ，…ビット分の情報量を備えた暗号鍵ｒを生成する（ステップＳ６）。送信側の通信装置は、この暗号鍵ｒを受信側の通信装置との共有鍵とする。

このように、本実施の形態においては、確定的で特性が安定した「Ｉｒｒｅｇｕｌａｒ－ＬＤＰＣ符号」用の検査行列を用いて受信データの誤りを訂正し、公開された誤り訂正情報に応じて共有情報の一部を捨てる構成とした。これにより、エラービットを特定／訂正するための膨大な回数のパリティのやりとりがなくなり、誤り訂正情報を送信するだけで誤り訂正制御が行われるため、誤り訂正処理にかかる時間を大幅に短縮できる。また、公開された情報に応じて共有情報の一部を捨てているので、高度に安全性の保証された共通鍵を生成することができる。

また、本実施の形態おいては、受信データの誤りを完全に訂正できるまで、符号化率を下げながらパリティ検査行列$H_{R(1)}$から所望のパリティ検査行列を抽出し、さらに追加のシンドロームを生成し、この追加シンドロームを用いて誤り訂正処理を繰り返し実行する構成とした。これにより、通信路の雑音レベルを見積もるために生成した共有情報を破棄する必要がなくなるので、共有鍵の生成効率を大幅に向上させることができる。

産業上の利用可能性

以上のように、本発明にかかる量子鍵配送方法および通信装置は、高度に安全性の保証された共通鍵を生成する技術として有用であり、特に、盗聴者が存在する可能性のある伝送路上の通信に適している。

請 求 の 範 囲

1． 量子通信路上の光子の測定結果として得られる確率情報付きの受信データの誤りを訂正することによって元の送信データを推定し、その推定結果を共有情報とする量子鍵配送方法において、

送信側および受信側の通信装置が、個別に、所望の範囲の符号化率で最適化された第１のパリティ検査行列（各装置で同一）を生成し、当該第１のパリティ検査行列から前記範囲内の特定の符号化率に対応した第２のパリティ検査行列（各装置で同一）を抽出する第１の検査行列生成ステップと、

前記送信側の通信装置が、前記第２のパリティ検査行列と前記送信データに基づいて生成した第１の誤り訂正情報を、公開通信路を介して前記受信側の通信装置に通知する第１の誤り訂正情報通知ステップと、

前記受信側の通信装置が、前記第１の誤り訂正情報に基づいて前記受信データの誤りを訂正する第１の誤り訂正ステップと、

前記受信データの誤りを完全に訂正できなかった場合に、受信側および送信側の通信装置が、個別に、前回の誤り訂正情報が次の誤り訂正時における情報の一部となるように、前記第１のパリティ検査行列から前回の符号化率よりも低い符号化率に対応した第３のパリティ検査行列（各装置で同一）を抽出する第２の検査行列生成ステップと、

前記送信側の通信装置が、前記第３のパリティ検査行列と前記送信データに基づいて生成した追加分の第２の誤り訂正情報を、公開通信路を介して前記受信側の通信装置に通知する第２の誤り訂正情報通知ステップと、

前記受信側の通信装置が、前記第１および第２の誤り訂正情報に基づいて前記受信データの誤りを訂正する第２の誤り訂正ステップと、

前記第１の誤り訂正ステップの処理で受信データの誤りを完全に訂正できた場合、または、前記第２の検査行列生成ステップ、前記第２の誤り訂正情報通知ステップ、前記第２の誤り訂正ステップの処理を繰り返し実行することにより誤り

を完全に訂正できた場合、公開された誤り訂正情報量に応じて共有情報の一部を破棄し、その結果を暗号鍵とする暗号鍵生成ステップと、

を含むことを特徴とする量子鍵配送方法。

2． 前記第１のパリティ検査行列の生成処理は、

符号長および前記所望の範囲の符号化率を決定する符号情報決定ステップと、

「行と列の重みが一定」かつ「２部グラフ上のサイクル数が６以上」を満たす前記第１のパリティ検査行列のベースとなる行列を選択し、当該行列に基づいて、前記範囲の上限値に対応した第１の基本行列、および前記範囲の下限値に対応した第２の基本行列を生成する基本行列生成ステップと、

前記符号長および前記符号化率の上限値に基づくガウス近似法の実行により、前記上限値に対応したパリティ検査行列の行の重みと列の重みの次数配分を最適化し、さらに当該次数配分に基づいて前記第１の基本行列の行重みおよび／または列重みを分割することにより、前記上限値に対応したパリティ検査行列を生成する検査行列生成ステップと、

「前記上限値に対応したパリティ検査行列を含むこと」という拘束条件の下で、前記符号化率の下限値に基づくガウス近似法を実行することにより、前記下限値に対応したパリティ検査行列の行の重みと列の重みの次数配分を最適化し、さらに当該次数配分に基づいて前記第２の基本行列の行重みおよび／または列重みを分割することにより、前記上限値に対応したパリティ検査行列に対する追加行列を生成する追加行列生成ステップと、

を含み、

前記上限値に対応したパリティ検査行列と前記追加行列とを連結した状態の前記下限値に対応したパリティ検査行列を、前記第１のパリティ検査行列とすることを特徴とする請求の範囲第１項に記載の量子鍵配送方法。

3． 前記第１のパリティ検査行列の生成処理は、

符号長および前記所望の範囲の符号化率を決定する符号情報決定ステップと、

「行と列の重みが一定」かつ「２部グラフ上のサイクル数が６以上」を満たす前記第１のパリティ検査行列のベースとなる行列を選択し、当該行列に基づいて、前記範囲の上限値に対応した基本行列、および前記範囲内で段階的に設定された複数の符号化率に対応した基本行列（前記範囲の下限値に対応した基本行列を含む）を生成する基本行列生成ステップと、

前記符号長および前記符号化率の上限値に基づくガウス近似法の実行により、前記上限値に対応したパリティ検査行列の行の重みと列の重みの次数配分を最適化し、さらに当該次数配分に基づいて、前記上限値に対応した基本行列の行重みおよび／または列重みを分割することにより、前記上限値に対応したパリティ検査行列を生成する検査行列生成ステップと、

「一段階上の符号化率に対応するパリティ検査行列を含むこと」という拘束条件の下で、前回よりも一段階下の符号化率に基づいてガウス近似法を実行することにより、当該符号化率に対応したパリティ検査行列の行の重みと列の重みの次数配分を最適化し、さらに当該次数配分に基づいて、前記一段階下の符号化率に対応した基本行列の行重みおよび／または列重みを分割することにより、前記一段階上の符号化率に対応したパリティ検査行列に対する追加行列を生成する追加行列生成ステップと、

を含み、

以降、前記符号化率を下げながら、前記下限値に対応する符号化率に達するまで、前記追加行列生成ステップを繰り返し実行し、

前記上限値に対応したパリティ検査行列およびすべての追加行列を連結した状態の前記下限値に対応したパリティ検査行列を、前記第１のパリティ検査行列とすることを特徴とする請求の範囲第１項に記載の量子鍵配送方法。

４．　前記「行と列の重みが一定」かつ「２部グラフ上のサイクル数が６以上」を満たす行列として、ユークリッド幾何符号を用いることを特徴とする請求の範

囲第２項に記載の量子鍵配送方法。

５．　前記「行と列の重みが一定」かつ「２部グラフ上のサイクル数が６以上」を満たす行列として、ユークリッド幾何符号を用いることを特徴とする請求の範囲第３項に記載の量子鍵配送方法。

６．　量子通信路上の光子の測定結果として得られる確率情報付きの受信データの誤りを訂正することによって元の送信データを推定し、その推定結果を送信側の通信装置との共有情報とする受信側の通信装置において、

所望の範囲の符号化率で最適化されたパリティ検査行列（以後、生成パリティ検査行列と呼ぶ）を生成し、当該生成パリティ検査行列から前記範囲内の所定の符号化率に対応したパリティ検査行列（以後、抽出パリティ検査行列と呼ぶ）を抽出する検査行列生成手段と、

前記抽出パリティ検査行列（各装置で同一）、送信側の通信装置から公開通信路を介して受け取る誤り訂正情報、に基づいて、前記受信データの誤りを訂正する復号手段と、

受信データの誤りを完全に訂正できた場合に、公開された誤り訂正情報量に応じて共有情報の一部を破棄し、その結果を暗号鍵とする暗号鍵生成手段と、

を備え、

前記検査行列生成手段が、

前記受信データの誤りを完全に訂正できなかった場合に、前記受信データの誤りを完全に訂正できるまで、前回の誤り訂正情報が次の誤り訂正時における情報の一部となるように、かつ符号化率を下げながら、前記生成パリティ検査行列から各符号化率に対応するパリティ検査行列（各装置で同一）を抽出し、

前記復号手段が、

送信側の通信装置から公開通信路を介して追加される誤り訂正情報に基づいて、前記受信データの誤りを訂正することを特徴とする通信装置。

7． 受信側の通信装置が量子通信路上の光子の測定結果として得られる確率情報付きの受信データから元の送信データを推定した場合に、その推定結果を受信側の通信装置との共有情報とする送信側の通信装置において、

所望の範囲の符号化率で最適化されたパリティ検査行列（以後、生成パリティ検査行列と呼ぶ）を生成し、当該生成パリティ検査行列から前記範囲内の所定の符号化率に対応したパリティ検査行列（以後、抽出パリティ検査行列と呼ぶ）を抽出する検査行列生成手段と、

前記抽出パリティ検査行列と前記送信データに基づいて誤り訂正情報を生成し、その生成結果を、公開通信路を介して前記受信側の通信装置に通知する誤り訂正情報生成手段と、

受信データの誤りが完全に訂正された場合に、公開した誤り訂正情報量に応じて共有情報の一部を破棄し、その結果を暗号鍵とする暗号鍵生成手段と、

を備え、

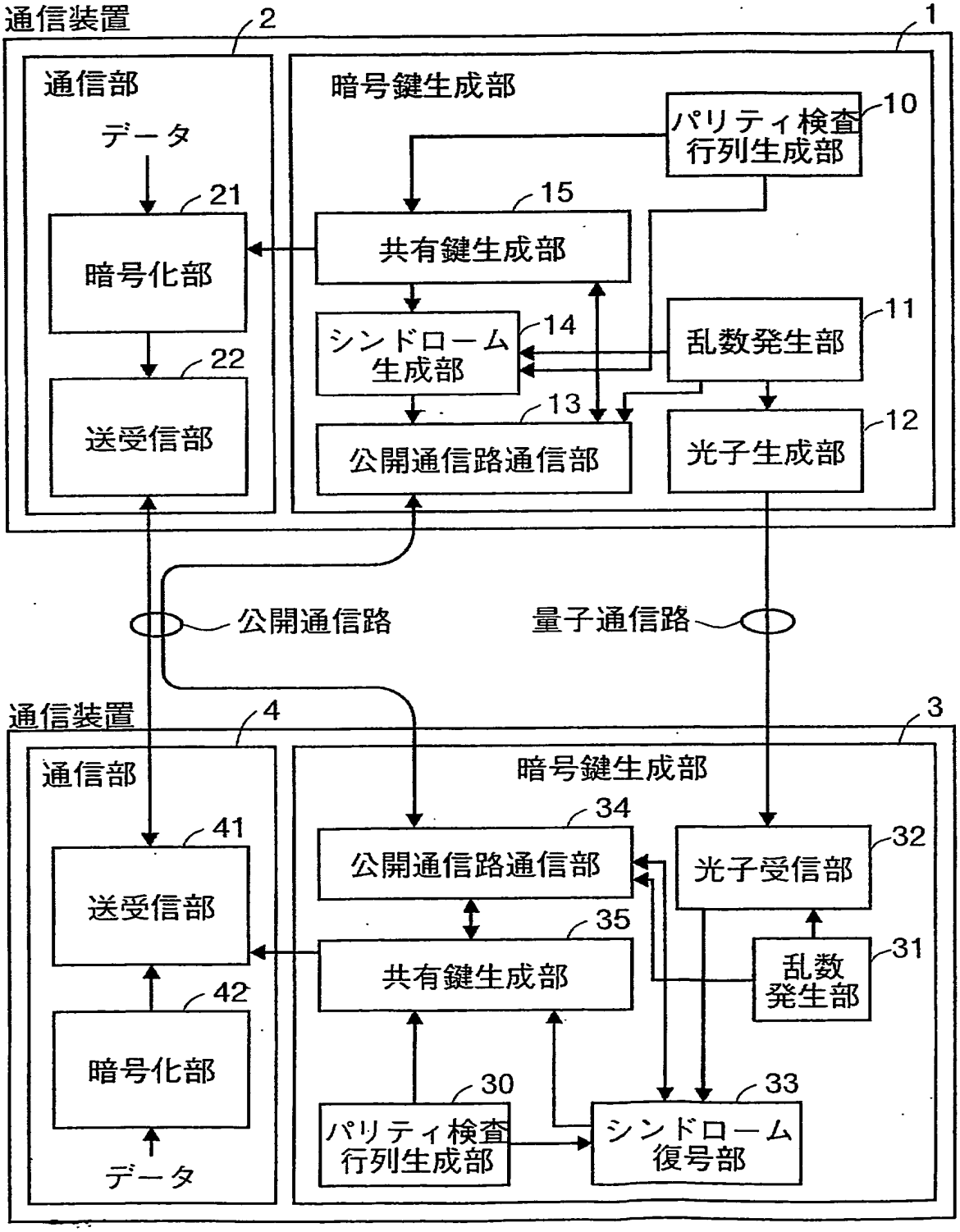
前記検査行列生成手段が、

前記受信データの誤りが完全に訂正されなかった場合に、前記受信データの誤りが完全に訂正されるまで、前回の誤り訂正情報が次の誤り訂正時における情報の一部となるように、かつ符号化率を下げながら、前記生成パリティ検査行列から各符号化率に対応するパリティ検査行列（各装置で同一）を抽出し、

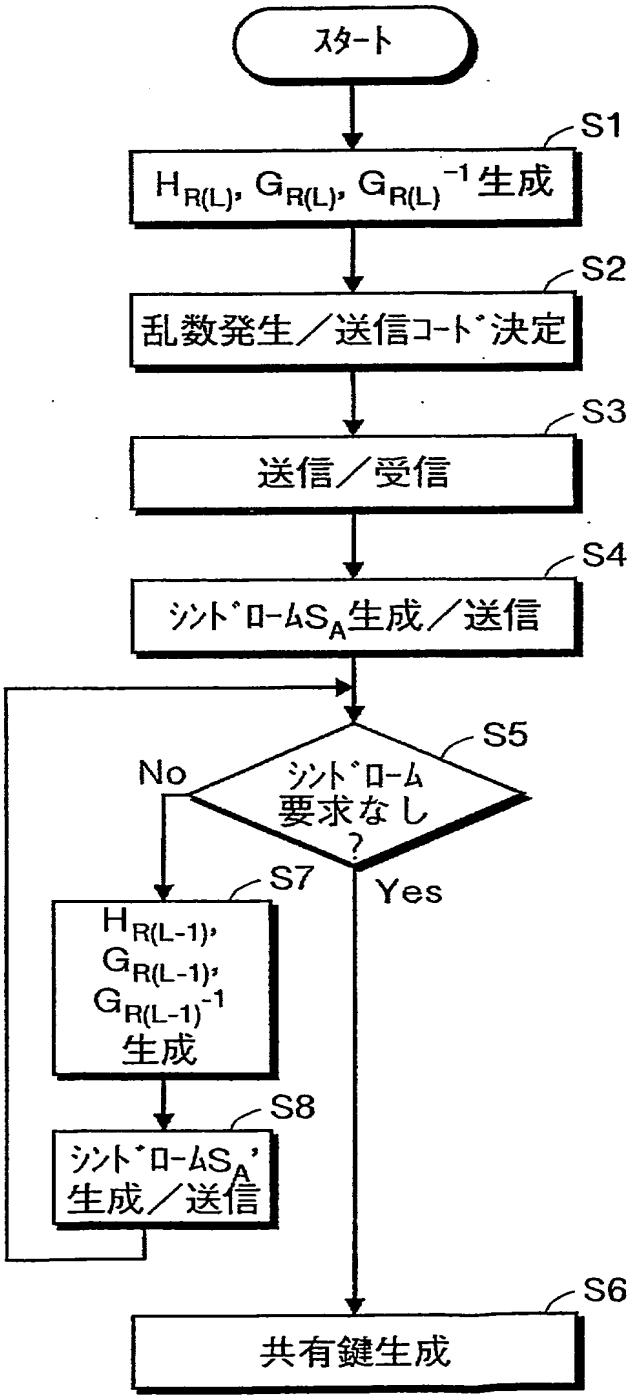
前記誤り訂正情報生成手段が、

前記受信データの誤りが完全に訂正されるまで、追加分の誤り訂正情報を、公開通信路を介して前記受信側の通信装置に通知することを特徴とする通信装置。

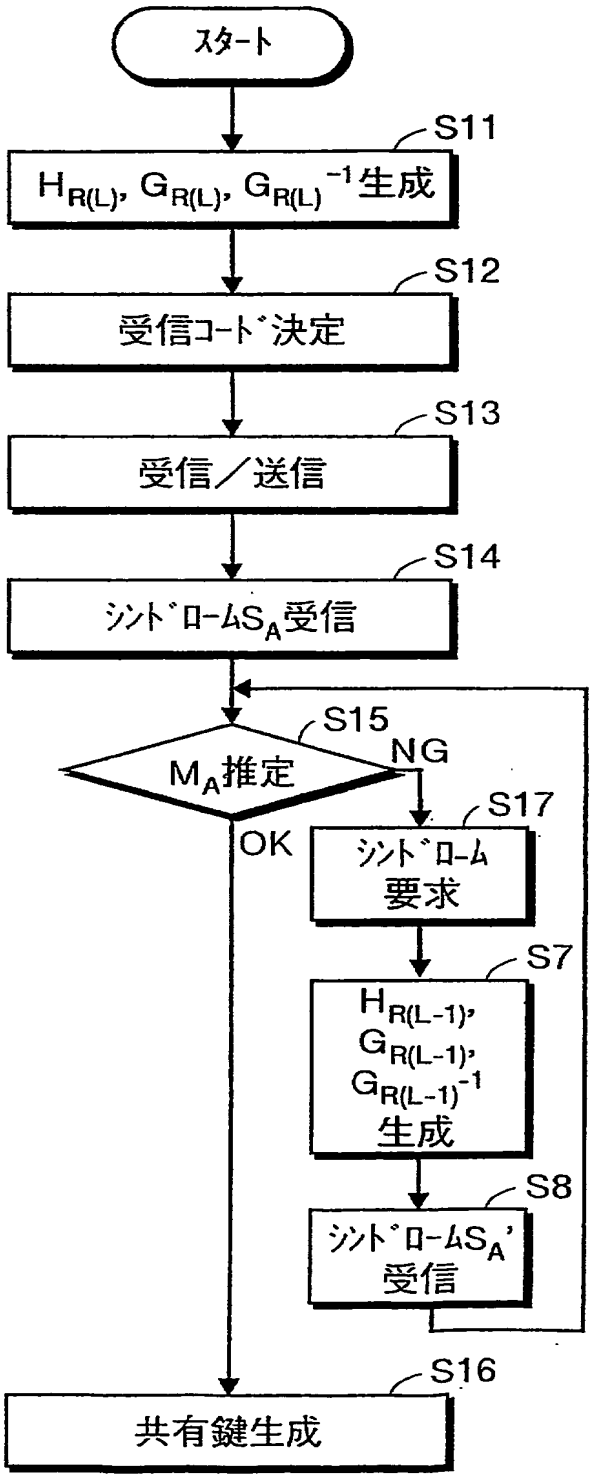
第1図


通信装置
2
1
通信部
データ
21
暗号化部
22
送受信部
暗号鍵生成部
パリティ検査
行列生成部
10
15
共有鍵生成部
シンドローム
生成部
14
乱数発生部
11
13
公開通信路通信部
光子生成部
12
公開通信路
量子通信路
通信装置
4
3
通信部
41
送受信部
42
暗号化部
データ
暗号鍵生成部
34
公開通信路通信部
光子受信部
32
35
共有鍵生成部
乱数
発生部
31
30
パリティ検査
行列生成部
33
シンドローム
復号部

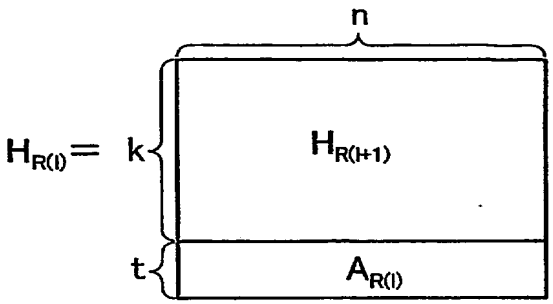
第2図


スタート
S1
$H_{R(L)}$, $G_{R(L)}$, $G_{R(L)}^{-1}$ 生成
S2
乱数発生／送信コード決定
S3
送信／受信
S4
シンドロームS_A生成／送信
S5
No
シンドローム要求なし？
Yes
S7
$H_{R(L-1)}$, $G_{R(L-1)}$, $G_{R(L-1)}^{-1}$ 生成
S8
シンドロームS_A'生成／送信
S6
共有鍵生成

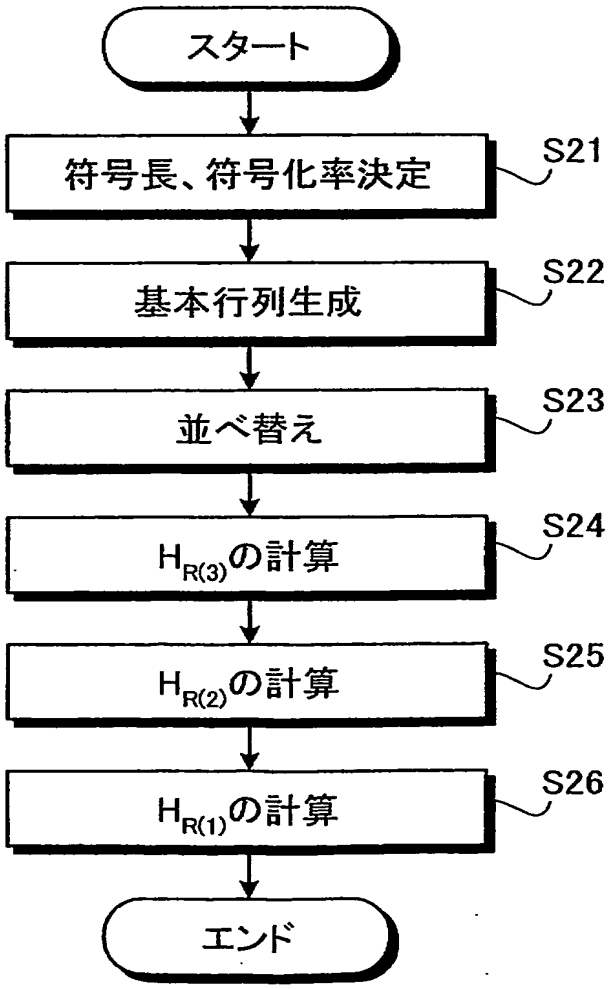
第3図


スタート
S11
$H_{R(L)}$, $G_{R(L)}$, $G_{R(L)}^{-1}$生成
S12
受信コード決定
S13
受信／送信
S14
シンドロームS_A受信
S15
M_A推定
NG
OK
S17
シンドローム要求
S7
$H_{R(L-1)}$, $G_{R(L-1)}$, $G_{R(L-1)}^{-1}$生成
S8
シンドロームS_A'受信
S16
共有鍵生成

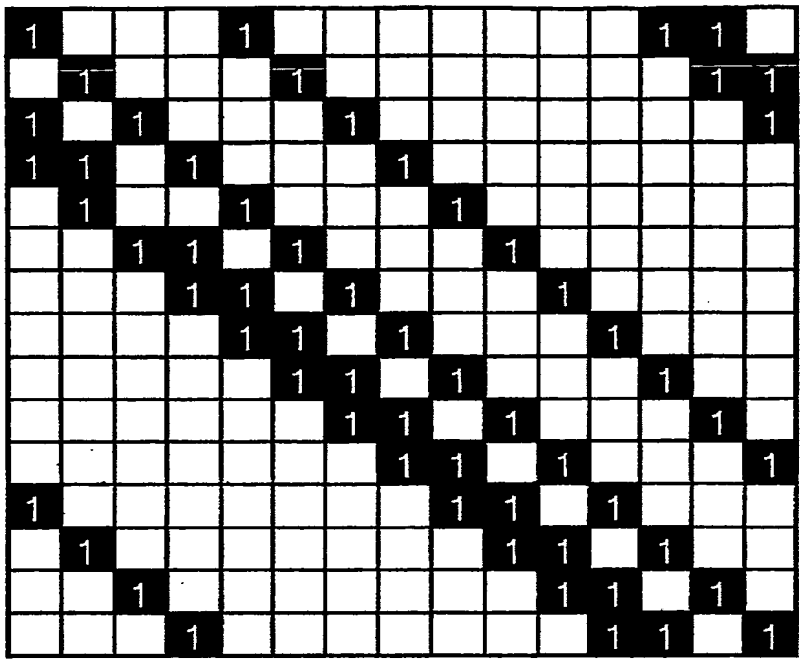
第4図


n
$H_{R(l)}$=
k
$H_{R(l+1)}$
t
$A_{R(l)}$

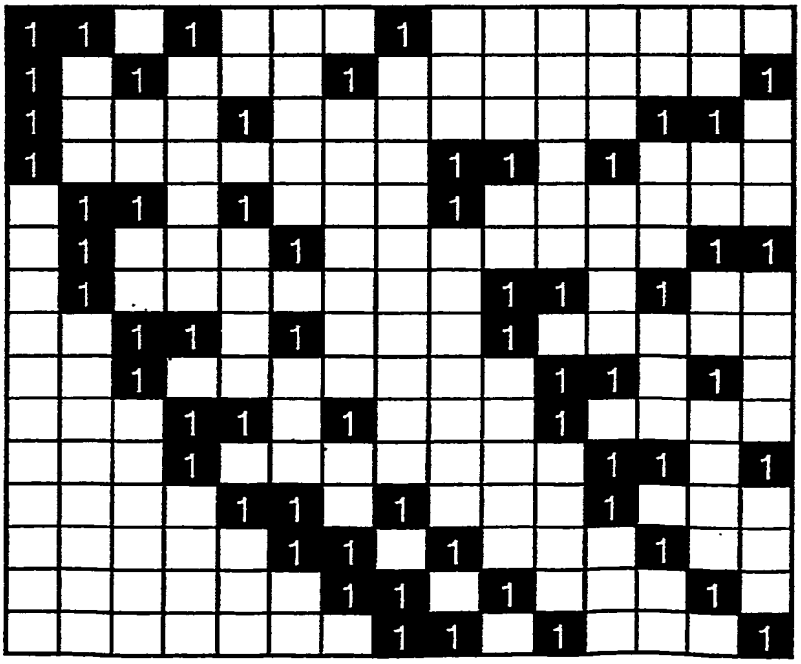
第5図


スタート
符号長、符号化率決定
S21
基本行列生成
S22
並べ替え
S23
$H_{R(3)}$の計算
S24
$H_{R(2)}$の計算
S25
$H_{R(1)}$の計算
S26
エンド

第6図



第7図



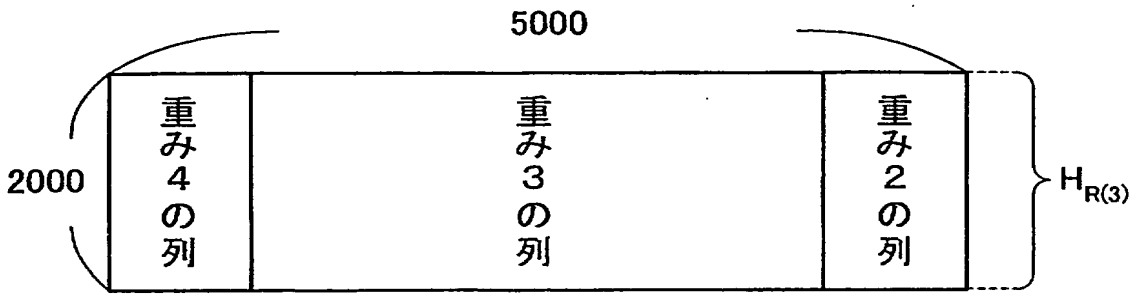
第8図

rate	rate=0.6
次数i	列次数比率 $\lambda_i(R(I))$
1	
2	0.01
3	0.970022733
4	0.019977267
次数i	行次数比率 $\rho_i(R(I))$
2	
7	7/15
8	8/15

第9図

	$H_{R(I)=0.6}$	
次数i	列次数比率 $\lambda_i(R(I))$	列数 $n_v(x,R(I))(m'=1000)$
1		
2	0.0372	279
3	0.8884	4442
4	0.0744	279
次数i	行次数比率 $\rho_i(R(I))$	行数 $n_c(x,R(I))(m'=1000)$
2		
3		
7	7/15	1000
8	8/15	1000

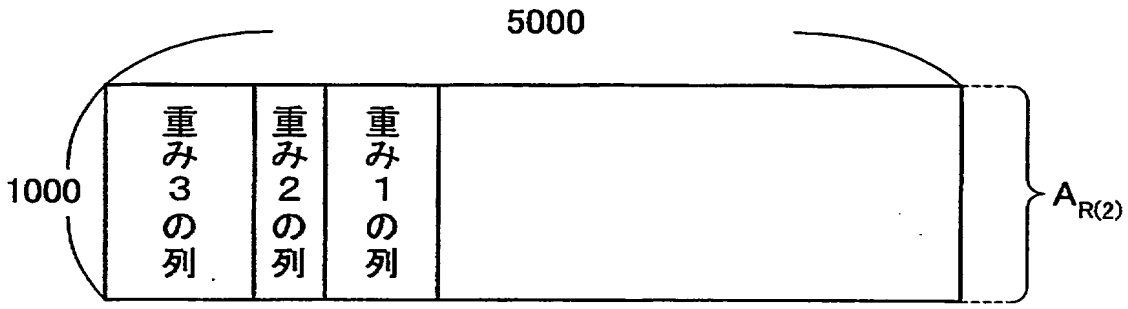
第10図



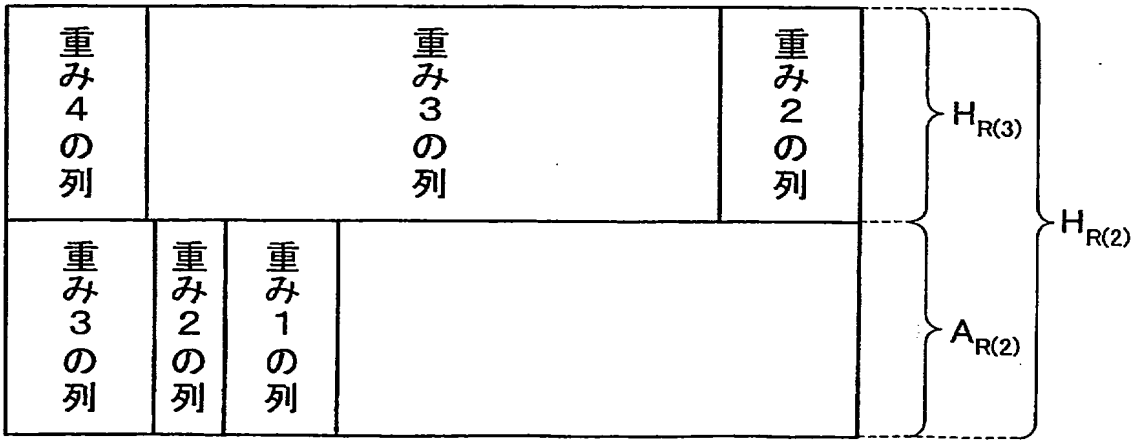
第11図

	$H_{R(l)=0.6}$		$H_{R(l-1)=0.4}$		$A_{R(l-1)=0.4}$
次数i	列次数比率 $\lambda_i(R(l))$	列数$n_v(x,R(l))$ (m'=1000)	列次数比率 $\lambda_i(R(l-1))$	列数$n_v(x,R(l-1))$ (m'=1000)	列数
1					150 $\lambda_3(R(l))$と同一の列:150
2	0.0372	279	0.0310	279	6 $\lambda_3(R(l))$と同一の列:6
3	0.8884	4442	0.6133	3619	946 $\lambda_4(R(l))$と同一の列:279 $\lambda_3(R(l))$と同一の列:667
4	0.0744	279	0.0333	150	
5			0.0017	6	
6			0.2833	667	
7			0.0373	279	
次数i	行次数比率 $\rho_i(R(l))$	行数$n_c(x,R(l))$ (m'=1000)	行次数比率 $\rho_i(R(l-1))$	行数$n_c(x,R(l-1))$ (m'=1000)	
2					
3			3/18	1000	
7	7/15	1000	7/18	1000	
8	8/15	1000	8/18	1000	

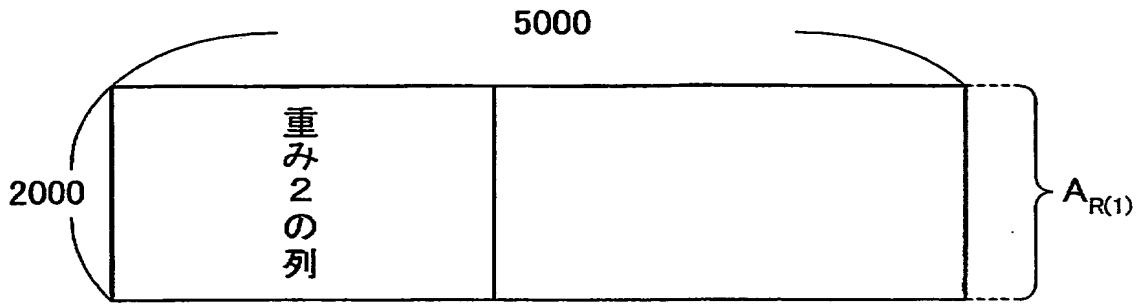
第12図


5000
1000
重み3の列
重み2の列
重み1の列
$A_{R(2)}$

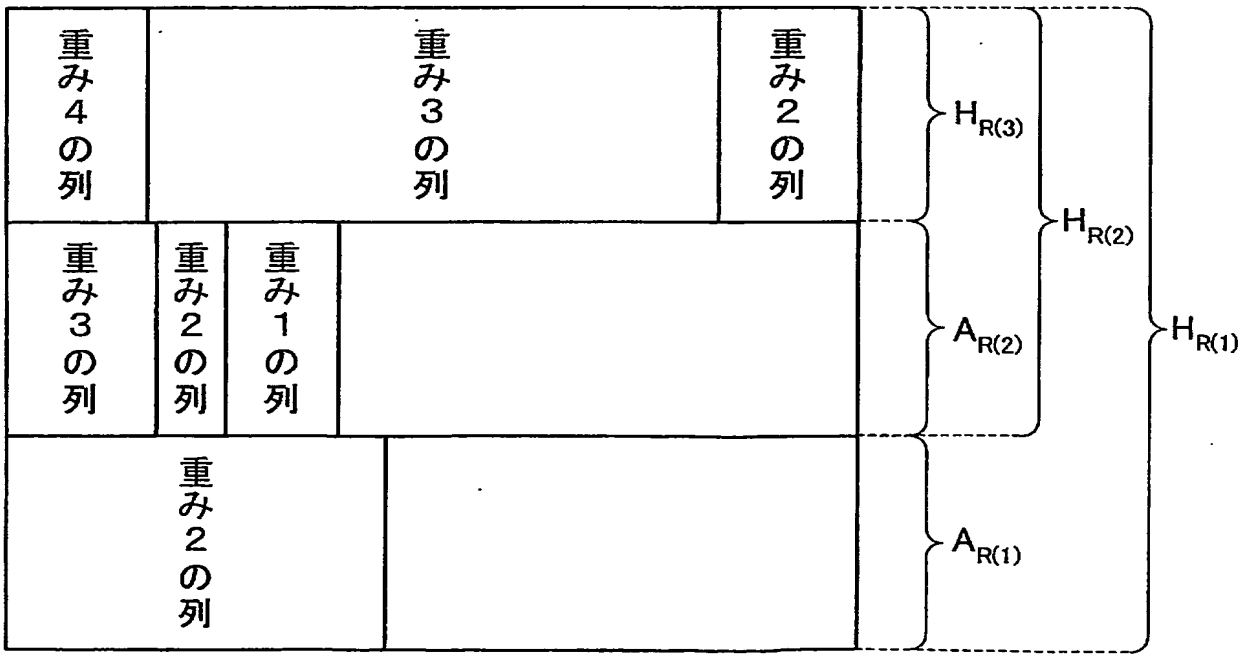
第13図


重み4の列
重み3の列
重み2の列
$H_{R(3)}$
$H_{R(2)}$
重み3の列
重み2の列
重み1の列
$A_{R(2)}$

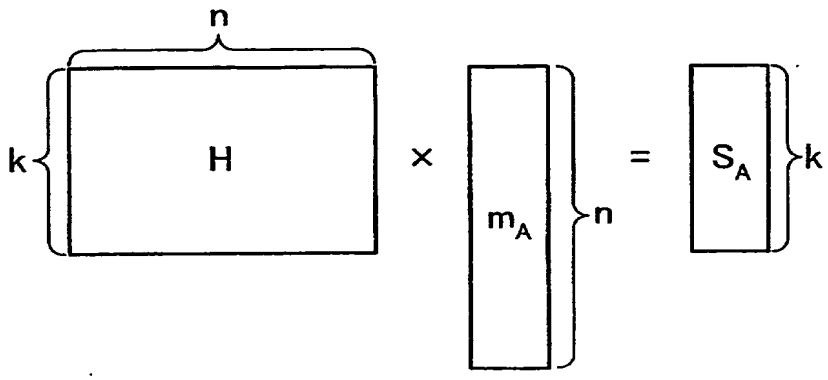
第14図


5000
2000
重み2の列
$A_{R(1)}$

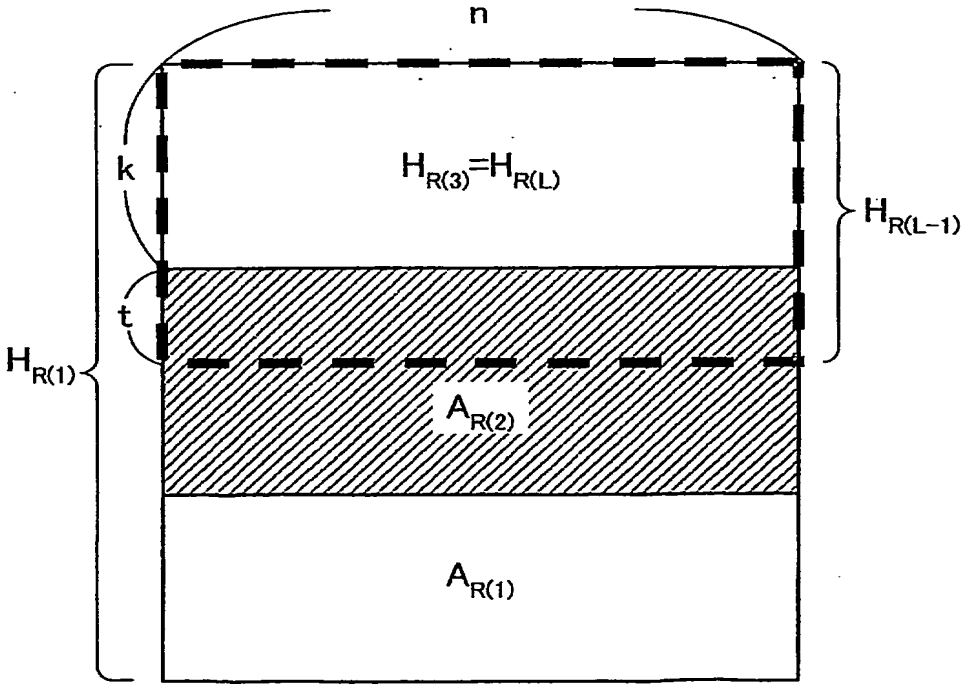
第15図


重み4の列
重み3の列
重み2の列
重み3の列
重み2の列
重み1の列
重み2の列
$H_{R(3)}$
$H_{R(2)}$
$A_{R(2)}$
$H_{R(1)}$
$A_{R(1)}$

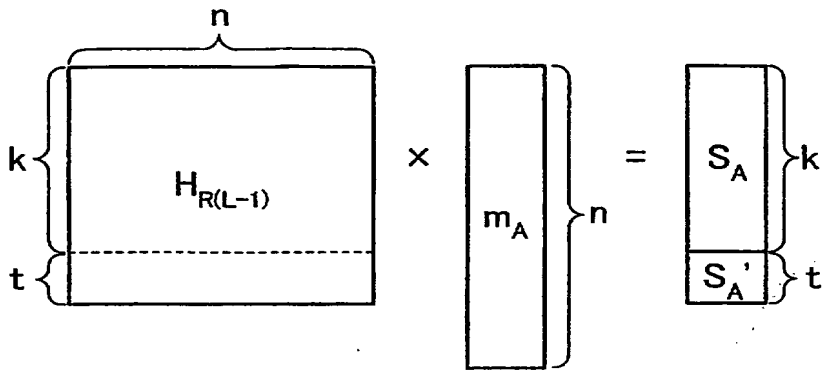
第16図



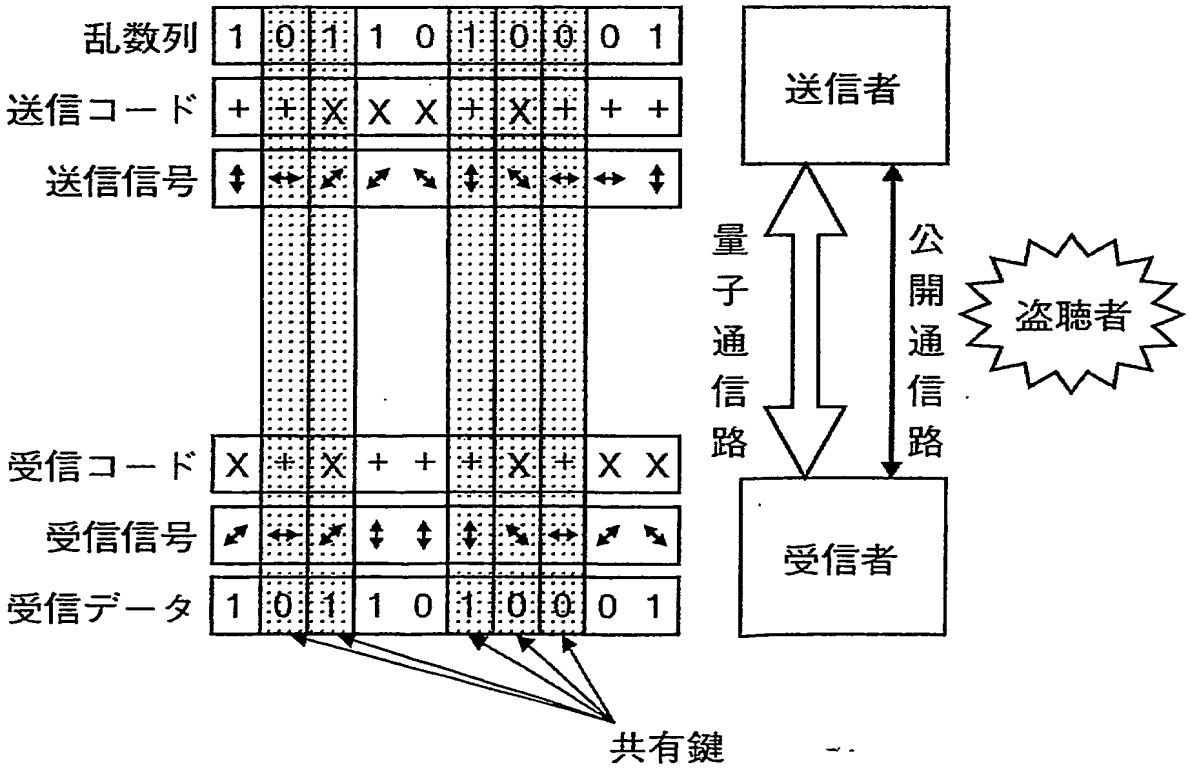
第17図



第18図


n
k
t
$H_{R(L-1)}$
×
m_A
n
=
S_A
k
S_A'
t

第19図


乱数列
送信コード
送信信号
受信コード
受信信号
受信データ
1 0 1 1 0 1 0 0 0 1
+ + X X X + X + + +
X + X + + + X + X X
1 0 1 1 0 1 0 0 0 1
送信者
受信者
量子通信路
公開通信路
盗聴者
共有鍵